DATE(S) ISSUED:
5/12/2010

SUBJECT:
Multiple Vulnerabilities in Adobe Shockwave Player Could Allow Remote Code Execution

OVERVIEW:
Multiple vulnerabilities have been discovered in Adobe Shockwave Player which could allow an attacker to take complete control of an affected system. Adobe Shockwave Player is a prevalent multimedia application used to display animations and video. These vulnerabilities may be exploited if a user visits or is redirected to a specifically crafted web page, or opens a specially crafted Shockwave (SWF) file. Successful exploitation may result in an attacker gaining the same privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

SYSTEMS AFFECTED:
> Adobe Shockwave Player 11.5.6.606 and prior

RISK:

Government:
> Large and medium government entities: **High**
> Small government entities: **High**

Businesses:
> Large and medium business entities: **High**
> Small business entities: **High**

Home users: High

DESCRIPTION:
Eighteen security vulnerabilities have been identified in Adobe Shockwave Player. These vulnerabilities may be exploited if a user visits or is redirected to a specifically crafted web page, or opens a specially crafted Shockwave (SWF) file.

The vulnerabilities are as follows:
> There are 16 memory corruption vulnerabilities that could result in remote code execution
> A denial-of-service vulnerability that is caused by an infinite loop.
> An unspecified integer-overflow vulnerability could result in remote arbitrary code execution.

Successful exploitation of the remote code execution vulnerabilities could result in an attacker gaining the same privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

RECOMMENDATIONS:
The following actions should be taken:
- Apply appropriate updates provided by Adobe to vulnerable systems immediately after appropriate testing.
- Do not open email attachments from unknown or un-trusted sources.

- Do not visit un-trusted websites or follow links provided by unknown or un-trusted sources.
- Inform and educate users regarding the threats posed by attachments and hypertext links contained in emails especially from un-trusted sources.

REFERENCES:

Adobe:
http://www.adobe.com/support/security/bulletins/apsb10-12.html

Security Focus:
http://www.securityfocus.com/bid/40082
http://www.securityfocus.com/bid/40083
http://www.securityfocus.com/bid/40088
http://www.securityfocus.com/bid/40089
http://www.securityfocus.com/bid/40090
http://www.securityfocus.com/bid/40091
http://www.securityfocus.com/bid/40093
http://www.securityfocus.com/bid/40094
http://www.securityfocus.com/bid/40096

CVE:
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0127
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0128
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0129
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0130
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0986
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0987
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-1280
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-1281
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-1282
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-1283
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-1284
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-1286
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-1287
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-1288
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-1289
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-1290
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-1291
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-1292

iDenfense Labs:
http://labs.idefense.com/intelligence/vulnerabilities/display.php?id=869

TippingPoint:
http://www.zerodayinitiative.com/advisories/ZDI-10-087
http://www.zerodayinitiative.com/advisories/ZDI-10-088
http://www.zerodayinitiative.com/advisories/ZDI-10-089